

Practical Advantages of Security, Education, and Awareness



2016 WV Cyber Security Conference



Opening Thoughts

Security awareness should not create such fear or angst that people are afraid to check e-mail or perform other legitimate business activities!

Agenda

Definitions

Why

Who

What

How

When

**Practical
Examples**

Q&A

Definitions

Definitions: Key terms

Education

Long term retention of facts or information

Training

Development of new skills or knowledge

Awareness

Increased perception of facts

Why

Why

- a) Compliance**
- b) Due care (legal protection)**
- c) Training is valuable**
- d) None of the above**
- e) All of the above**

Opening Thoughts

Security awareness should produce culture whereby employees behave well when they encounter security opportunities in the workplace.

Why

A strong security culture is just as important as an aware workforce.

Who

Who

Everyone should be considered.

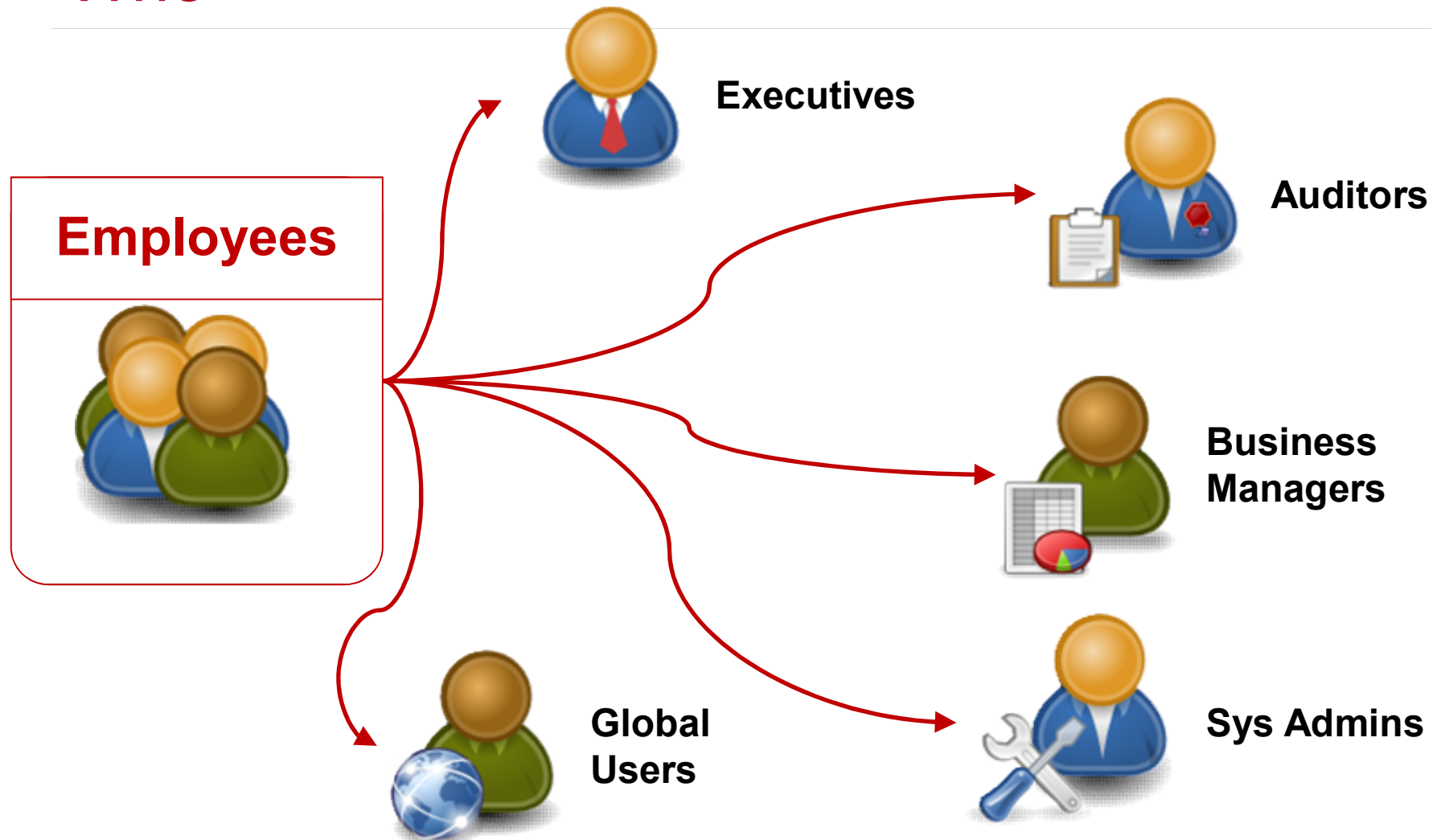
Employees

Partners

Vendors




Customers

Who



What

What

-  **Set strong passwords of sufficient complexity and length.**
-  **Don't use the same password on all your accounts**
-  **Don't share passwords with anyone**

What



Keep your operating system, browser and other critical software optimized by installing updates



Limit the amount of personal information you share online



Use privacy settings to avoid sharing information widely

What

Tailor the training

Recommendations and content should be tailored to address the risks faced by distinct types of users.

What

Executives

Spear phishing (whaling) and other targeted attacks

IT

Domain credentials and privileged file execution

General Users

Drive-by downloads, fraud, and general attacks of convenience.

What

Reinforce policies

Do not miss an opportunity!
**Use this time to reinforce policies
and standards.**

How

How: Education and Training

Computer-based training (CBT)

Instructor-led training

Third-party facilitation

Self-directed training

How: Awareness

Practical exercises

Relevant updates

Posters

E-mail

When

When

- 1. Initial training for new users**
- 2. At least annually**
- 3. Related to significant changes
(*often overlooked*)**

Practical Examples

Practical Examples

Rewards Drive Behavior

For \$12,000 per year, you can revolutionize engagement and build a hyper-aware workforce with small cash bonuses for organizational compliance.

Practical Examples

Consideration Drives Behavior

You can increase awareness by redacting user-specific data and sharing real threat intel to discourage participation in active attacks.

Q&A

Contact

Keyaan Williams

Senior Consultant

Risk Management & Governance

[https://www.nccgroup.trust/us/
Keyaan.Williams@nccgroup.trust](https://www.nccgroup.trust/us/Keyaan.Williams@nccgroup.trust)

